

# Next Generation Secure Computing Base

Paul England, John Manferdelli, Marcus Peinado  
Security Business Unit  
Microsoft Corporation

**The Past is Prologue**

# Computer Security 101 – The Standard Model

# Computer Security 101 – The Standard Model

- Establish Security Perimeter around Trusted Computing Base (“TCB”) usually during boot

# Computer Security 101 – The Standard Model

- Establish Security Perimeter around Trusted Computing Base (“TCB”) usually during boot
- Authenticate security principals within security perimeter

# Computer Security 101 – The Standard Model

- Establish Security Perimeter around Trusted Computing Base (“TCB”) usually during boot
- Authenticate security principals within security perimeter
- Authorize or deny actions based on security principal and access rules naming principal

# Computer Security 101 – The Standard Model

- Establish Security Perimeter around Trusted Computing Base (“TCB”) usually during boot
- Authenticate security principals within security perimeter
- Authorize or deny actions based on security principal and access rules naming principal
- Use cryptographic techniques for verifying identity, and protecting integrity and confidentiality of data and rules outside security perimeter



# Software acts on our behalf

- Our reliance on software is increasing
- You can't beat software for flexibility and features
- Current OSs are brittle and have enormous TCBs
- Trust relationships are complex, dynamic and ephemeral
- We have few tools to ensure it's working in our best interest



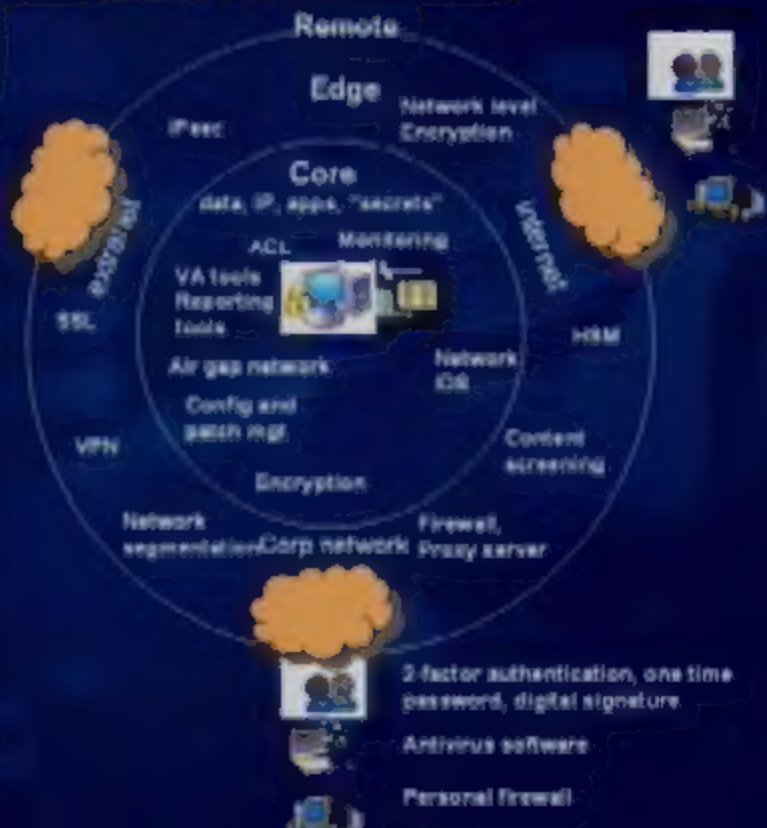
# Software acts on our behalf

- Our reliance on software is increasing
- You can't beat software for flexibility and features
- Current OSs are brittle and have enormous TCBs
- Trust relationships are complex, dynamic and ephemeral
- We have few tools to ensure it's working in our best interest

# The Modern Problem

"Using encryption on the Internet is the equivalent of arranging an armored car to deliver credit-card information from someone living in a cardboard box to someone living on a park bench."

Professor  
Gene Spafford  
Purdue  
GERIAS



# Hobson's Choice

● The **Entire Quid system package** establishes Security.

# Hobson's Choice

- **Closed System**

- Entire hardware package establishes Security Perimeter

- Only software approved by device Manufacturer.

- Fixed function

- Small TCB

# Hobson's Choice

## ● Closed System

- Entire hardware package establishes Security Perimeter
- Only software approved by device Manufacturer.
- Fixed function
- Small TCB

## ● Open System

- General Purpose
- Big TCB
- Permeable
- Lots of flexibility

We pick "both"



# **We pick “both”**

## ● **Trusted Open System**

- ❑ **Dynamically erected Security Perimeter**
- ❑ **“Effective TCB” for critical operations is small**
- ❑ **High security assurance (perimeter integrity, authentication reliability, authorization flexibility)**
- ❑ **Any OS and any application can run**
- ❑ **General Purpose**
- ❑ **Behavior is predictable even under adversarial software attack.**



# **We pick “both”**

## ● **Trusted Open System**

- **Dynamically erected Security Perimeter**
- **“Effective TCB” for critical operations is small**
- **High security assurance (perimeter integrity, authentication reliability, authorization flexibility)**
- **Any OS and any application can run**
- **General Purpose**
- **Behavior is predictable even under adversarial software attack.**

# Next Generation Secure Computing Base

Thanks to MSR: This represents work of MSR and MSR alums including Butler Lampson, John Detreville, Paul and John with help from Dan Simon, MSR Crypto and others at MSR.

# Next Generation Secure Computing Base Defined

- Microsoft's Next-Generation Secure Computing Base (NGSCB) is a bad name for a new security technology for the Microsoft Windows platform
  - Uses a unique hardware and software design
  - New kind of security model for integrity, confidentiality and trust negotiation in an interconnected world

# NGSCB Security Goals

- Protect data and processing against software attacks

# NGSCB Security Goals

- Protect data and processing against **software attacks**
- Provide a strong way to authenticate machines and software.

# NGSCB Security Goals

- Protect data and processing against **software attacks**
- Provide a strong way to authenticate machines and software.
- Provide "compartmentalization" of secure applications
  - Small, dynamically materialized security perimeters with unspoofable TCBs

# NGSCB Security Goals

- Protect data and processing against **software attack**
- Provide a strong way to authenticate machines and software.
- Provide "compartmentalization" of secure applications
  - ↳ Small, dynamically materialized security perimeters with unspoofable TCBs
- Provide safe haven in "network rich" environment



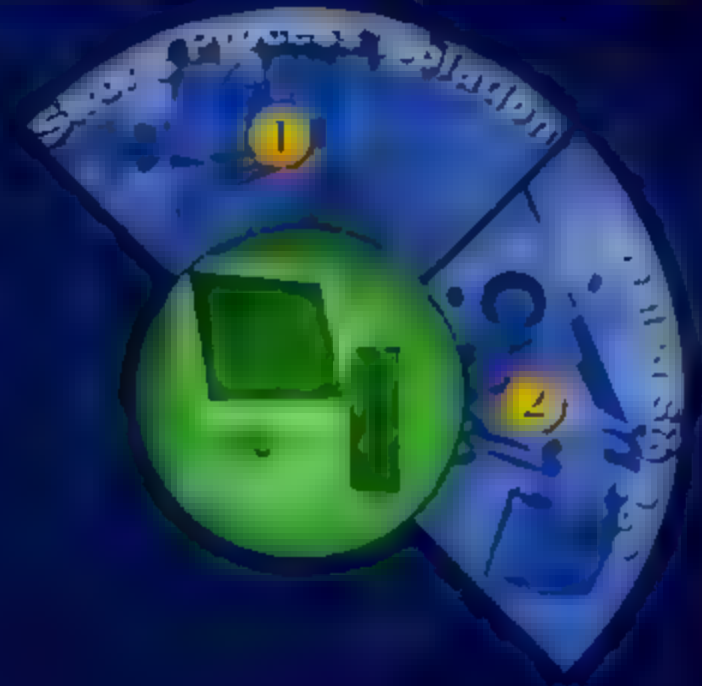
# Key NGSCB Components



# Key NGSCB Components



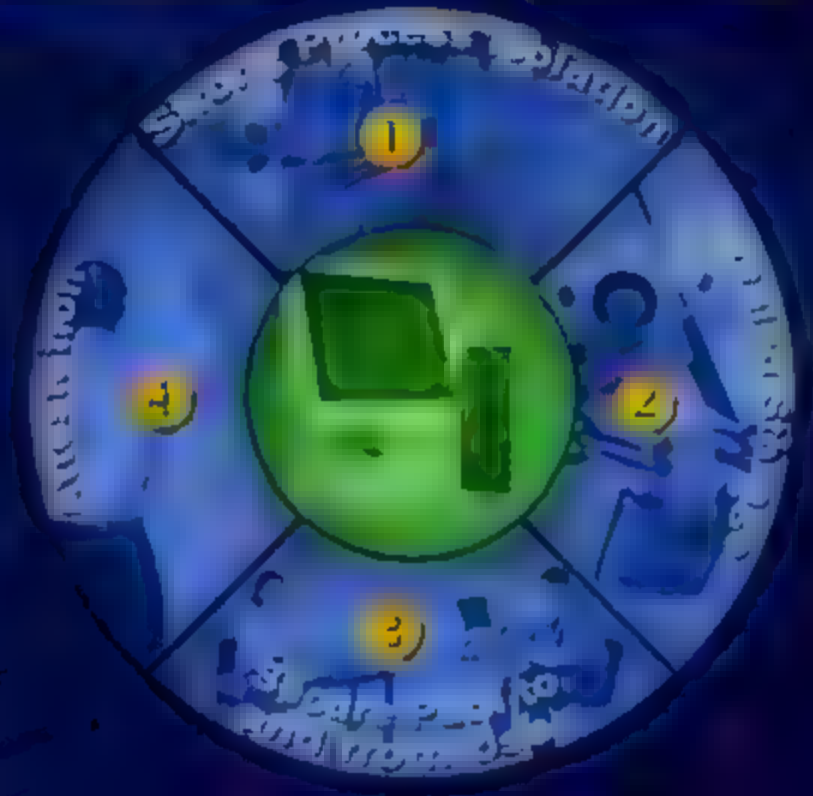
# Key NGSCB Components



# Key NGSCB Components



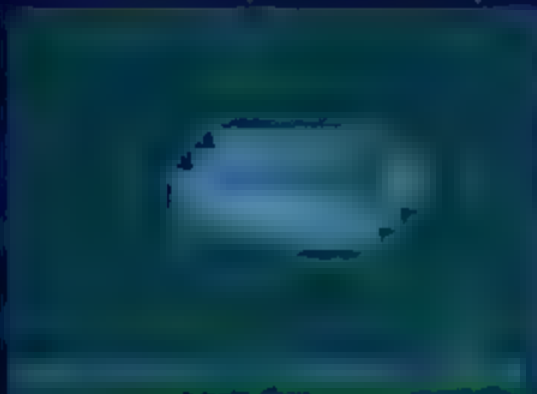
# Key NGSCB Components



# NGSCB Quadrants

Standard-Mode ("std-mode"/LMS)

User



Kernel



Hardware



# NGSCB Quadrants

Standard-Mode ("std-mode"/LHS)

Neuro-Mode (RHS)

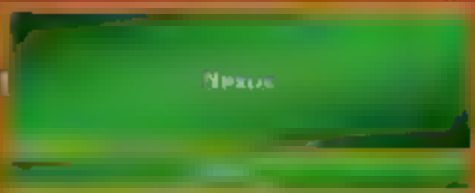
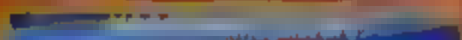
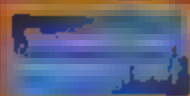
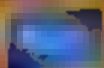
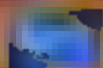
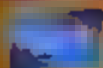
User



Workflow



Hardware





# Attestation extends TCB

Attestation is a process by which a system can prove to a remote party that it is running a specific version of a software component, and that the component is not tampered with.

Attestation is a process by which a system can prove to a remote party that it is running a specific version of a software component, and that the component is not tampered with.

Attestation is a process by which a system can prove to a remote party that it is running a specific version of a software component, and that the component is not tampered with.

Attestation is a process by which a system can prove to a remote party that it is running a specific version of a software component, and that the component is not tampered with.

Attestation is a process by which a system can prove to a remote party that it is running a specific version of a software component, and that the component is not tampered with.

Attestation is a process by which a system can prove to a remote party that it is running a specific version of a software component, and that the component is not tampered with.

Attestation is a process by which a system can prove to a remote party that it is running a specific version of a software component, and that the component is not tampered with.

Attestation is a process by which a system can prove to a remote party that it is running a specific version of a software component, and that the component is not tampered with.

Attestation is a process by which a system can prove to a remote party that it is running a specific version of a software component, and that the component is not tampered with.

# NGSCB Quadrants

Standard-Mode ("std-mode" / LHS)

News-Mode (RHS)

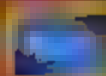
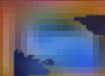
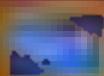
User



Kernel



Hardware



# Attestation extends TCB

- Program generates public/private key pair

# Attestation extends TCB

- Program generates public/private key pair
- Platform signs statement "The following public key is in an isolated program with hash H under Nexus N."
  - Another program can rely on without a central authority
  - Don't try this at home, safe pi more complicated
  - May be replaced by Zero Kn Protocol

# Attestation extends TCB

- Program generates public/private key pair
- Platform signs statement "The following public key is in an isolated program with hash H under Nexus N."
- Another program can rely on this key without a central authority
- Don't try this at home, safe protocol is more complicated
- May be replaced by Zero Knowledge Protocol

# Attestation Caveat

- Attestation is NOT a judgment of code quality or fitness
  - Code could still be malicious
  - Code could still have bugs affecting security
- Attestation leaves judgment up to challenger
  - Done with high confidence

# What Runs On The LHS

- Windows as you know it today
- Applications and Drivers still run
- Viruses too
- Any software with minor exceptions
  - ✱ The new hardware (HW) memory controller won't allow certain "bad" behaviors, e.g., code which
    - ✱ Puts the CPU into real mode



# What the RHS Needs From The LHS

- Memory Management changes to allow nexus to participate in memory pressure and paging decisions
- Window Manager coordination
- IPC, scheduling, communication
- NGSCB management software and services

# Business Scenarios

Secure Distribution

Secure Distribution

Secure Distribution

Secure Distribution

Secure Distribution

Secure Distribution

Secure Distribution

Secure Distribution

# Business Scenarios

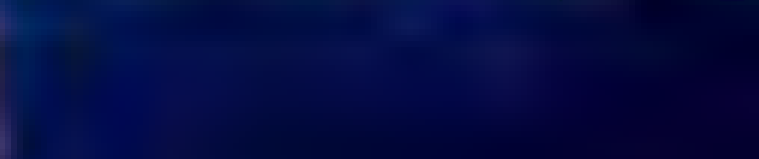
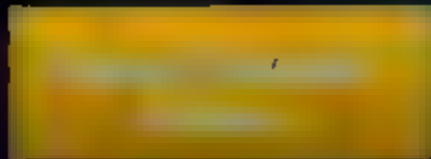
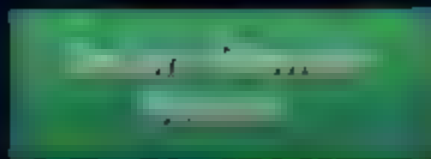
Secure Distribution

Secure Access

Secure Processing

Secure Distribution Processing

# Business Scenarios



# Business Scenarios



2000-2005

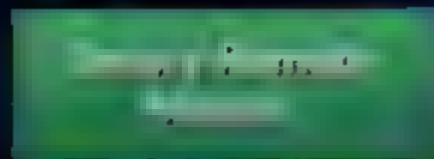
2000-2005  
Policy

Beauve Distribution Program



2000-2005  
Policy

# Business Scenarios



## Business Scenarios



# Business Scenarios

Business Scenario 1

Business Scenario 2

Business Scenario 3

Business Scenario 4

Business Scenario 5

Business Scenario 6

Business Scenario 7

Business Scenario 8



# Business Scenarios

Scenario 1: Market Expansion

Scenario 2: Product Diversification

Scenario 3: Strategic Alliances

Scenario 4: Digital Transformation

Scenario 5: Globalization

Scenario 6: Sustainability Initiatives

# Business Scenarios

## Confidentiality Enforcement

- Protect data on user machine
- Protect spoofed machines and users
- Provide Secure Audit

## "Small" Rights Management

- Protect personal data at Amazon
- Secure RMS from software attack
- Protect Corporate Partner Information

## "Big" Rights Management

- Books, movies, audio, software
- Flexible use models: Differential pricing
- Content not "orphaned" by new devices

## Secure Collaboration

# Business Scenarios

## Confidentiality Enforcement

- Protect data on user machine
- Protect spoofed machines and users
- Provide Secure Audit

## "Small" Rights Management

- Protect personal data at Amazon
- Secure RMS from software attack
- Protect Corporate Partner Information

## "Big" Rights Management

- Books, movies, audio, software
- Flexible use models: Differential pricing
- Content not "orphaned" by new devices

## Secure Collaboration

# Business Scenarios

## Confidentiality Enforcement

- Protect data on user machine
- Protect spoofed machines and users
- Provide Secure Audit

## "Small" Rights Management

- Protect personal data at Amazon
- Secure RMS from software attack
- Protect Corporate Partner Information

## "Big" Rights Management

- Books, movies, audio, software
- Flexible use models: Differential pricing
- Content not "orphaned" by new devices

## Secure Collaboration

- Auctions
- Negotiations
- On-line Games

# NGSCB: Threat Models

- **Our Threat Model**
  - No Software-Only Attacks Against RHS
  - No Break-Once/Break-Everywhere (BOBE) attacks
- **No Software-Only Attacks means...**
  - No attacks based on micro-code, macro-code, adapter card scripts, etc.
  - Any attacks launched from the Web or e-mail are "software only"
- **Protection only applies to the release of secrets**